SYSTEM FOR SECURING THE CONFIDENTIALITY OF ELECTRONICALLY STORED DATA IN THE EVENT OF THE PHYSICAL THEFT THEREOF

Origin of the Invention

The invention described herein was made in the performance of official duties by an employee of the Department of the Navy and may be manufactured, used, licensed by or for the Government for any governmental purpose without payment of any royalties thereon.

Cross-reference to Related Patent Applications

This patent application is co-pending with one related patent application entitled "DATA INFLATION FOR MASKING VALUABLE DATA" (Navy Case No. 96150), by the same inventor as this patent application.

Field of the Invention

The invention relates generally to security systems for electronic data, and more particularly to a system that provides for the electronic storage of data and for security of the confidentiality thereof in the event that the system and/or stored data is physically removed or stolen from an authorized location.

Background of the Invention

Companies, organizations and civilian/military government entities often have electronic data repositories for storage of critical and/or sensitive data. The data repositories can be static storage facilities for archiving data storage devices, or dynamic storage facilities that provide for the electronic transfer of data into and out of

data storage devices. In either case, the data storage devices are typically maintained in a physical location that is secured utilizing one or more conventional "secure facility" systems such as locked rooms/buildings, security checks for personnel having authorized access to the secure facility, alarm systems, etc. However, if access is gained to the secure facility, it is often easy to physically remove or steal the data storage devices maintained in the secure facility. Given the current state-of-the-art in data storage device capacity, it is conceivable that one individual can walk off with large amounts of critical and/or sensitive data in a coat pocket. Once in possession of these data storage devices, the thief can access the secret or confidential data thereon at his leisure using his own processing equipment. Even if the stored confidential data is encrypted for security, most (if not all) encryption routines can be "cracked" given enough time and sufficient computing power.

Summary of the Invention

Accordingly, it is an object of the present invention to provide a system for securing the confidentiality of electronically stored data in the event of a physical theft thereof.

Other objects and advantages of the present invention will become more obvious hereinafter in the specification and drawings.

In accordance with the present invention, a system secures the confidentiality of data stored in data storage devices. A position determination system is mechanically coupled to the data storage devices and continuously determines a position thereof. A processor is electrically coupled to the data storage devices and the position

determination system. The processor is further provided with an authorized location for the data storage devices. The processor facilitates transfer of data to and from the data storage devices. More specifically, when the position of the data storage devices matches the authorized location, the processor facilitates transfer of data from the data storage devices without any modification of the data. However, when the position of the data storage means does not match the authorized location, the processor modifies the data transferred from the data storage devices by (i) parsing the data to be transferred from the data storage devices into constituents thereof, and (ii) randomly incorporating the constituents into a set of irrelevant data having storage requirements that exceed those of the data to be transferred by a plurality of orders of magnitude.

The system can further include sensors coupled to the data storage devices for sensing attempts to physically move the data storage means devices. Should this happen, the sensors generate a control signal that is used to activate a self-destruction system coupled to the data storage devices. Still further, the system can include alarms and/or a transmitter. The alarms can be activated when the position of the data storage devices does not match the authorized location and/or when the sensors detect movement of the data storage devices. The transmitter wirelessly transmits the position of the data storage devices when the position of the data storage devices does not match the authorized location and/or when the sensors detect movement of the data storage devices.

Brief Description of the Drawings

Other objects, features and advantages of the present

invention will become apparent upon reference to the following description of the preferred embodiments and to the drawings, wherein corresponding reference characters indicate corresponding parts throughout the several views of the drawings and wherein:

FIG. 1 is a block diagram of one embodiment of a system for securing the confidentiality of electronically stored data in the event of a physical theft thereof in accordance with the present invention;

FIG. 2 is another embodiment of the present invention that includes a self-destruct mechanism used to secure the confidentiality of the data in the event that attempts are made to remove the system's data storage device(s) from the system; and

FIG. 3 is still another embodiment of the present invention that includes alarm(s) and/or a transmitter for generating alarm(s) and/or position signals, respectively, in the event of a physical theft of the entire system or if attempts are made to remove the system's data storage device(s).

Detailed Description of the Invention

Referring now to the drawings, and more particularly to FIG. 1, a block diagram of a first embodiment of a system for securing the confidentiality of electronically stored data in the event of a physical theft thereof in accordance with the present invention is shown and is referenced generally by numeral 10. As used herein, the term "physical theft" refers to a physical taking by which the system and/or the device(s) used to electronically store data are physically moved from their intended or authorized location.

System 10 includes one or more data storage devices 12,

a position determination system 14 attached or otherwise mechanically coupled to data storage device(s) 12, and a data transfer processor 16 having a data inflation processing scheme programmed therein. Data storage device(s) 12 can be any data storage medium used to electronically store data. Such data storage media include but are not limited to chip-based read only memory (ROM) or random access memory (RAM), magnetic disks, compact disks (CDs), digital video disks (DVDs), etc. Further, a variety of format(s) can be used to store and/or encrypt the stored data without departing from the scope of the present invention.

Position determination system 14 will generally include a Global Positioning System (GPS) receiver, and can include localized position determination devices such as an inertial system or ring laser gyro element.

Data transfer processor 16 can be any type of processor that can be used to control the transfer of data to and from data storage device(s) 12. In general, data transfer processor 16 controls authorized data transfers to and from data storage device(s) 12 in any of a variety of ways that would be well understood in the art. In addition, data transfer processor 16 is programmed with one or more "data inflation" schemes that greatly inflates stored data that is being electronically extracted/copied from device(s) 12 in the event of unauthorized removal or physical theft of system 10.

Briefly, a "data inflation" scheme referred to herein modifies the data as it is being extracted/copied (from data storage device(s) 12) by (i) dividing or parsing the data being extracted/copied into its constituent parts with the size of the parts being the same or different; and (ii) randomly incorporating the constituent parts into a very

large set of irrelevant data that can be generated in real-time by data transfer processor 16.

In general, the size of a constituent part of the data should be small enough such that it does not represent any recognizable part of the data. The size of the set of irrelevant data is preferably substantially larger (i.e., a number of orders of magnitude) than the size of the data being extracted/copied. For example, each kilobyte of stored data being extracted/copied could be divided up and intermixed (by data transfer processor 16) with 100 gigabytes of irrelevant data generated by data transfer processor 16. This means that a 1 megabyte stored data file would generate 100,000 gigabytes of inflated data. Note that the actual amount of data inflation could be more or less than this example without departing from the scope of the present invention.

The particular scheme used to generate a large, irrelevant data set is not a limitation of the present invention as any one of a number of such schemes could be used herein without departing from the scope of the present invention. For example, a large irrelevant data set of numbers could be generated using a system calendar and clock maintained on data transfer processor 16. More specifically, assume that I is an elapsed time in seconds from some arbitrary start time on a system clock and D is a number of days since some reference date. A simple algorithm could then be used to generate a large set of random numbers using D and I. For example, one could start with some transcendentally-derived number such as the D-th root of "pi" raised to the I-th power. The system would then mix each digit of the stored data with a different 10^8 digits (i.e., 100 gigabytes) of the generated irrelevant data set. Another

way of generating the irrelevant data set would be to take the D-th root of an arbitrary irrational number raised to the I-th power. Data inflation could be completed by converting the stored data to numbers and randomly inserting same into the generated set of irrelevant (number) data.

Data inflation as described herein serves two purposes. First, the time/bandwidth requirements for downloading enormous data files will greatly tax an unauthorized user or thief's system. Second, the large set of generated irrelevant data will mask the real data which has been parsed into constituent parts. Thus, even if a thief has the capability to download and store the inflated data, it must then be "deflated" and have the data of interest separated from the irrelevant data.

In operation, data transfer processor 16 is provided or programmed with one or more authorized locations. Position determination system 14 continuously determines its position and, therefore, the position of data storage device(s) 12. The determined position is compared with the authorized location(s). A match between the two means that system 10 and data storage device(s) 12 are where they should be. In such a case, requests for data (which, for purposes of the present invention, are assumed to be properly authorized) are handled by data transfer processor 16 without any data modification. However, if there is disagreement between the authorized location(s) and the determined position, data transfer processor 16 implements its data inflation scheme for any subsequent data extraction/copying attempts.

It is possible that a thief may attempt to just take data storage device(s) 12. This may be especially true where the system to which the data storage device(s) are coupled is too large/heavy to be moved from its authorized location.

For example, FIG. 2 illustrates a system 20 that includes a platform 22 (e.g. cabinet, floor, shelf, etc.) to which data storage device(s) 12, position determination system 14 and, optionally, data transfer processor 16 are mechanically coupled. Each of device(s) 12, system 14 and processor 16 operates as described hereinabove. System 20 further includes one or more sensors 24 coupled to data storage device(s) 12 for sensing any attempts to remove device(s) 12 from platform 22. Accordingly, sensors 24 can include motion sensors, contact switches, and combinations thereof, to detect such removal attempts. In the event that a removal attempt is detected, sensors 24 generate a control signal used to activate a self-destruct mechanism 26 coupled to data storage device(s) 12. Self-destruct mechanism 26 can be configured to, upon activation, destroy one or both of data storage device(s) 12 and the data stored thereon. The type of self-destruct mechanism can be any of a variety of such mechanisms without departing from the scope of the present invention. For example, if device(s) 12 are a magnetic storage media, self-destruct mechanism 26 might be an electromagnet. Other possibilities for self-destruct mechanism 26 include, but are not limited to, small incendiary devices that can burn or melt device(s) 12 or the storage media, a pressurized container of corrosive or highly oxidizing fluid or gas, a binary explosive system in which components react when brought into contact with one another, or a mechanical device designed to scratch the storage media beyond readability.

Another option is to encase system 20 in a secure container or vault 28 so that theft of system 20 essentially requires theft of the entirety of vault 28. Still further, for blast and/or fire protection, the sides, top and bottom

of vault 28 can have blast and heat shields 28A affixed thereto.

Still another embodiment of the present invention is shown in FIG. 3 where a system 30 includes all of the elements of system 20 (to optionally include vault 28 with shields 28A), and further includes one or more alarms 32 and a transmitter 34. Alarms 32 can be coupled to data transfer processor 26 for activation when data storage device(s) 12 are not in an authorized location. Additionally or alternatively, alarms 32 can be coupled to sensors 24 for activation when sensors 24 detect any attempt to remove data storage device(s) 12 from platform 22 and/or vault 28. The types of alarms 32 can include one or more of audio alarms, video alarms, and "silent" alarms that are audible/visible at a remote location, without departing from the scope of the present invention. Transmitter 34 can be coupled to data transfer processor 16 to transmit the position determined by system 14. The transmission is preferably a wireless transmission. The position transmission could occur continuously, periodically, or only when system 30 is not in an authorized location or when sensors 24 detect an attempt to remove data storage device(s) 12 from platform 22. Thus, system 30 not only secures the confidentiality of data stored on device(s) 12, but also provides the means to retrieve a stolen system 30 and, possibly, provide the authorities with the means to apprehend those responsible for such theft or attempted theft.

The advantages of the present invention are numerous. The system secures the confidentiality of stored data when the entire system is moved from an authorized location. Further, the system secures the confidentiality of stored data when attempts are made to steal just the devices on

which the data is stored.

Although the invention has been described relative to a specific embodiment thereof, there are numerous variations and modifications that will be readily apparent to those skilled in the art in light of the above teachings. It is therefore to be understood that, within the scope of the appended claims, the invention may be practiced other than as specifically described.

What is claimed as new and desired to be secured by Letters Patent of the United States is: